Identity Theft Prevention Plan
Revised 9/8/08

For the protection of our customers, and in compliance with the Federal Trade Commission, Hickory Telephone Company and HTC Communications (collectively HTC) have implemented an Identity Theft Prevention Plan. In accordance with this plan:

- New applicants are required to present:
  - Two valid forms of ID
  - Social Security Number
- A credit report will be run on all new applicants.
- Our current CPNI policy will be followed (Appendix A), ensuring that only the account holder or those designated by the account holder may make changes to the account.
- Employees will be instructed to be alert for "Red Flags", which are indicators of identity theft.

Red Flags

HTC employees should be alert for the following "red flags", identified by the Federal Trade Commission (FTC), indicating possible identity theft. If the employee encounters a case of possible fraud, the employee should bring the issue to the immediate attention of management.

Alerts, Notifications, or Other Warnings Received from Consumer Reporting Agencies or Service Providers, Such as Fraud Detection Services

1. A fraud or active duty alert is included with a consumer report.

   - Detection: Employees will review the report and determine which, if any customers or applicants are involved.
   - Response: Accounts suspected of fraud will be suspended while the matter is investigated. New accounts will be denied. Law enforcement will be contacted as necessary.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

   - Detection: Employees will review the report and determine which, if any customers or applicants are involved.
   - Response: Accounts suspected of fraud will be suspended while the matter is investigated. New accounts will be denied. Law enforcement will be contacted as necessary.

3. A consumer reporting agency provides a notice of address discrepancy.

- Detection: Employees will review the report and determine which, if any customers or applicants are involved.
- Response: Accounts suspected of fraud will be suspended while the matter is investigated. New accounts will be denied. Law enforcement will be contacted as necessary.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

   a. A recent and significant increase in the volume of inquiries;

   b. An unusual number of recently established credit relationships;

   c. A material change in the use of credit, especially with respect to recently established credit relationships; or

   d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

- Detection: Employees will review the report and determine which, if any customers or applicants are involved
- Response: Accounts suspected of fraud will be suspended while the matter is investigated. New accounts will be denied. Law enforcement will be contacted as necessary.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

   - Detection: Employees should scan identification documents for anything out of the ordinary.
   - Response: If there is a question about validity, the employee should require that the customer provide an additional form of ID. If the customer is unable to provide a valid form of ID, service should be denied. Law enforcement will be contacted as necessary.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

   - Detection: Employees should scan the photo or description on the ID to make sure it is consistent with the appearance of the applicant.
   - Response: If there is a question about validity, the employee should require that the customer provide an additional form of ID. If the customer is unable to

provide a valid form of ID, service should be denied. Law enforcement will be contacted as necessary.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

- Detection: Employees should scan identification documents for an inconsistent address, social security number, signature, or other information.
- Response: If there is a question about validity, the employee should require that the customer provide an additional form of ID. If the customer is unable to provide a valid form of ID, service should be denied. Law enforcement will be contacted as necessary.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

- Detection: If the applicant was a previous customer, employees should compare the information in our billing system with the information provided by the applicant.
- Response: If an inconsistency occurs, service should be denied unless a valid explanation is given for the inconsistency. (A valid explanation would include a change of address, indicating the applicant has moved). Law enforcement will be contacted as necessary.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

- Detection: Employees should scan the application for anything out of the ordinary.
- Response: Service should be denied. Law enforcement will be contacted as necessary.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

    a. The address does not match any address in the consumer report; or

- Detection: The applicant's information should be compared with that in the report.
- Response: Service will be denied unless applicant presents a valid reason for the discrepancy. Law enforcement will be contacted as necessary.

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

- Detection: A credit check run on the applicant indicates an inconsistency.
- Response: Service should be denied unless a valid explanation is given for the inconsistency. Law enforcement will be contacted as necessary.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

- Detection: Employees should scan identification documents for inconsistencies.
- Response: If there is a question about validity, the employee should require that the customer provide an additional form of ID. If the customer is unable to provide a valid form of ID, service should be denied. Law enforcement will be contacted as necessary.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or
b. The phone number on an application is the same as the number provided on a fraudulent application.

- Detection: Any fraudulent activity that is detected will be kept in a log, accessible to customer service employees. Information provided by the applicant should be scanned to ensure it does not match information in the log.
- Response: Service should be denied. Law enforcement will be contacted as necessary.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or prison; or
b. The phone number is invalid, or is associated with a pager or answering service.

- Detection: Any fraudulent activity that is detected will be kept in a log, accessible to customer service employees. Information provided by the applicant should be scanned to ensure it does not match information in the log.
- Response: Service should be denied. Law enforcement will be contacted as necessary.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

    - Detection: A credit check run on the applicant indicates an inconsistency.
    - Response: Service should be denied. Law enforcement will be contacted as necessary.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

    - Detection: N/A
    - Response: N/A

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

    - Detection: The applicant will be required to complete the application.
    - Response: Service should be denied if the applicant refuses.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

    - Detection: If the applicant was a previous customer, employees should compare the information in our billing system with the information provided by the applicant.
    - Response: If an inconsistency occurs, service should be denied unless a valid explanation is given for the inconsistency. Law enforcement will be contacted as necessary.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

    - Detection: N/A
    - Response: N/A

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional, or replacement cards or a cell phone, or for the addition of authorized users on the account.

    - Detection: N/A

- Response: N/A

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

    a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (*e.g.*, electronics equipment or jewelry); or

- Detection: N/A
- Response: N/A

    b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

- Detection: N/A
- Response: N/A

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

    a. Nonpayment when there is no history of late or missed payments;

- Detection: Employees should be alert for this situation when recording non-payments.
- Response: The customer should be contacted. If the customer cannot be reached or a valid explanation is not provided, the account should be suspended. Law enforcement will be contacted as necessary.

    b. A material increase in the use of available credit;

- Detection: N/A
- Response: N/A

    c. A material change in purchasing or spending patterns;

- Detection: N/A
- Response: N/A

    d. A material change in electronic fund transfer patterns in connection with a deposit account; or

- Detection: N/A
- Response: N/A

    e. A material change in telephone call patterns in connection with a cellular phone account

- Detection: N/A
- Response: N/A

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

    - Detection: N/A
    - Response: N/A

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

    - Detection: N/A
    - Response: N/A

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

    - Detection: N/A
    - Response: N/A

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

    - Detection: HTC's CPNI policy specifies that only the account holder or authorized individuals can make changes to the account.
    - Response: Other individuals will not be allowed to make changes to the account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

    - Detection: The company will notify law enforcement of the claim.
    - Response: The company will comply with any requests made by law enforcement.

This plan will be updated as needed to reflect changes in risks to customers based on experiences of the company, changes in methods of identity theft, changes in methods to

detect, prevent and mitigate identity theft, changes in types of accounts offered and maintained, or changes in business arrangement including mergers, acquisition or joint ventures, and service provider arrangements.

Prepared by: Terri Jeffers

Signature: Terri Jeffers

Date: 9/18/08

The plan's administrator will be responsible for:

- Instructing employees in the implementation of the program
- Ensuring that employees are properly carrying out the steps of the program
- Periodically reviewing the log of fraudulent activity recorded by employees
- Determining when the policy needs to be updated
- Approving updates to the program
- Presenting annual reports to the board of directors which include material matters related to the program such as effectiveness, the risk of identity theft in connection with the opening of new accounts and with regard to existing accounts, any incidents involving identity theft and management's response, and any recommendations for material changes.

Administrator: _____

Signature: Greg Adamson

Date: 9/18/08

This plan has been reviewed and approved by the HTC board of directors.

Signature (Officer): Kathleen Jamison

Date: 9/18/08

Signature (Secretary): Paul J. Thies

Date: 9/18/08

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

ANNUAL § 64.2011 CPNI CERTIFICATION

FOR CALENDAR YEAR 2017

FCC FORM 499 FILER ID: 809742
HICKORY TELEPHONE COMPANY

FCC FORM 499 FILER ID: 814747
Advanced Telephone Systems, Inc
DBA - ATS Mobile Communications
DBA – HTC Communications

EB Docket No. 06-36

---

75 Main Street
Hickory, PA 15340
Phone: (724) 356-2211
Fax: (724) 356-4398

/Users/tlj/Documents/Documents - Terri Jeffers's MacBook Pro/HTC/misc/policies that must be reviewed annually/CPNI/2017CPNI Policy.doc

I. Introduction

Hickory Telephone Company, on behalf of itself and its affiliate HTC Communications (individually or collectively "the Company"), hereby submits its 2017 CPNI compliance certificate in accordance with § 64.2009(e) of the Commission's rules.

II. Statement of Compliance with CPNI Requirements

The Company has implemented operating procedures and safeguards to ensure compliance with 47 CFR §64.2005 - §64.2009. To this end, the Company has procedures in place which ensure that:

- CPNI is not shared with any affiliates unless that affiliate already provides service to the customer,
- CPNI is not shared with any third parties absent a court order or subpoena,
- CPNI is not used in any outbound telemarketing campaigns,
- Procedures are in place to notify customers if CPNI is going to be used or otherwise disclosed, and there is a process in place to allow individual customers to "opt out" of this use,
- Procedures (**passwords**) are in place to authenticate the identity of callers to the business office before any CPNI is discussed,
- Formal training is provided by the Company on CPNI regulations and the related procedures in place to ensure compliance. (**Meet regularly with employees to review procedures**)

III. Actions Taken Against Data Brokers

The Company has not taken any actions against data brokers in the past year. The Company understands that it must report on any information it has with respect to the processes pretexters are using to attempt to access CPNI, and what steps the Company is taking to protect CPNI.

IV. Consumer Complaints Regarding Unauthorized Release of CPNI

The Company has not received any customer complaints in the past year concerning the unauthorized release of CPNI. The following table illustrates this point, and will be used by the Company on an ongoing basis to track CPNI customer complaints for both internal purposes and FCC reporting.

Consumer Complaint Summary by Complaint Type – 2017	
Type of Consumer Complaint	***Complaints***
Improper access by employees	0
Improper disclosure to individuals not authorized to receive the information	0
Improper access to online information by individuals not authorized to view the information	0
Total Consumer Complaints	0

V. Certification

I, Terri Jeffers, certify that I am an officer of the Company named above, and acting as an agent of the Company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq*.

I have undertaken an investigation, with assistance from personnel within our company, of the procedures related to CPNI acquisition, storage, protection, use, and customer permission to use data of the Company. Section II of this certification includes a statement explaining how the Company's procedures ensure compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules. Based upon my personal investigation, it is my opinion that the operating procedures of the Company are in compliance with the Commission's CPNI rules as outlined in 47 CFR §64.2005 - §64.2009.

I state under penalty of perjury that the foregoing is true and correct.

Officer Name: Terri Jeffers

Officer Title: Regulatory Director

Signature: Terri Jeffers, Regulatory Director

Date: Febuary 21, 2018

/Users/tlj/Documents/Documents - Terri Jeffers's MacBook Pro/HTC/misc/policies that must be reviewed annually/CPNI/2017CPNI Policy.doc

- I ackowledge that I have reviewed the company's CPNI policy as set forth:

- A password must be established to access customer call detail records over the phone
  - Call detail = the number called, the time of the call, location of the call, duration of the call.
  - If the customer does not know their password, CSR's may call the telephone number on file (but may only speak with the account holder or a person previously designated by the account holder). It can also be mailed to the address on file (must have been on file for 30 days). If they come in person, CSR's may ask for ID. Name and address on the ID must match that on the account.
  - If a customer mentions certain information, you may talk about the information that the customer has stated, even if they do not have a password, but only that particular information.
  - Business customers – information can be given to the name on the account (after authentication). If there is no name on the account, CPNI may be mailed to the address on file, or we can call the number on file.

- Any other requests for information (including TV and Internet services) must still be authenticated. If a CRS does not personally know the person, they must ask for account number (not phone number) and the customer must verify the balance on their last bill. If they come in to the office, they may show ID.

- Only the account holder, or those specified by the account holder may make changes to the account
  - Postcards must be mailed out if someone changes their address or password (postcard would be mailed to the previous address).

- We will not share information about customer accounts outside of Hickory Telephone Company and/or HTC Communications (HTC affiliates). However, we may share this information between the two. The customer has the right to instruct us not to share CPNI between HTC affiliates by contacting us at 724-356-2211 or sending a letter to HTC - 75 Main St. Hickory, PA. Customers are notified annually of this policy. They are also notified when they establish service.
  - CPNI opt out is listed under "Occupation" as no share. If they have opted out, CSR's may not talk to them about HTC Communications services (long distance, TV, Internet) unless they already have services from HTC Communications.

- In the case of a breach, Secret Service and FBI must be contacted via the web portal at www.fcc.gov/eb/cpni in no later than 7 days.
  - The customer must be notified 7 days AFTER law enforcement is advised.
  - The customer may be notified sooner, only in a case where irreparable harm would come to the customer if they were notified later.
  - Records must be kept for 2 years.

HTC SM Hickory Telephone Co.
75 Main Street • Hickory, PA • 15340 • 724-356-2211 • FAX: 724-356-4398

- I acknowledge that I have reviewed the 2017 Consumer Complaint Summary.

Consumer Complaint Summary by Complaint Type – 2017	
Type of Consumer Complaint	***Complaints***
Improper access by employees	0
Improper disclosure to individuals not authorized to receive the information	0
Improper access to online information by individuals not authorized to view the information	0
Total Consumer Complaints	0

Name: [signature] Date: 2/20/18

Name: [signature] Date: 2-20-18

Name: [signature] Date: 2/20/18

Name: [signature] Treas Date: 2-20-18

HTC Hickory Telephone Co.
75 Main Street • Hickory, PA • 15340 • 724-356-2211 • FAX: 724-356-4398

Identity Theft Prevention - Red Flag Report

In compliance with Federal Trade Commission rules, this report details the status of the Identity Theft Prevention Plan, signed into effect on September 10, 2008 by Hickory Telephone Company and HTC Communications (collectively HTC).

A. Effectiveness of HTC's policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts
   a. Since the plan's implementation, there have been no known incidents of identity theft or other breach of customer security. This includes both new and existing accounts.
   b. Employees have been trained to follow the procedures outlined in the Identity Theft Prevention Plan. HTC employees have the tools necessary to detect and handle any breaches of security that may occur in the future.

B. Service provider arrangements
   a. No arrangements have been made.

C. Significant incidents involving identity theft and management's response
   a. No incidents have occurred.

D. Recommendations for significant changes to the program.
   a. No changes are recommended at this time.

Administrator: Terri Jeffers

Signature: Terri Jeffers, Regulatory Director

Date: 2/21/18